Terms used: **key password multiple several different** Found **2,945** of **216,412**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 Cryptography and data security
Dorothy Elizabeth Robling Denning
January 1982 Book
Publisher: Addison-Wesley Longman Publishing Co., Inc.
Full text available: pdf(19.47 MB) Additional Information: full citation, abstract, references, cited by, index terms

From the Preface (See Front Matter for full Preface)

Electronic computers have evolved from exiguous experimental enterprises in the 1940s to prolific practical data processing systems in the 1980s. As we have come to rely on these systems to process and store data, we have also come to wonder about their ability to protect valuable data.

Data security is the science and study of methods of protecting data in computer and communication systems from unauthorized disclosure ...

2 Macintosh human interface guidelines
Apple Computer, Inc.
January 1992 Book
Publisher: Addison-Wesley Publishing Company
Full text available: pdf(37.61 MB) Additional Information: full citation, abstract, references, cited by, index terms

Macintosh Human Interface Guidelines describes the way to create products that optimize the interaction between people and Macintosh computers. It explains the whys and hows of the Macintosh interface in general terms and specific details.

Macintosh Human Interface Guidelines helps you link the philosophy behind the Macintosh interface to the actual implementation of interface elements. Examples from a wide range of Macintosh products show good human interface design, including individ ...

3 A framework for password-based authenticated key exchange[1]
Rosario Gennaro, Yehuda Lindell
May 2006 **ACM Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 2
Publisher: ACM Press
Full text available: Additional Information:

pdf(574.64 KB) full citation, abstract, references, index terms

In this paper, we present a general framework for password-based authenticated key exchange protocols, in the common reference string model. Our protocol is actually an abstraction of the key exchange protocol of Katz et al. and is based on the recently introduced notion of smooth projective hashing by Cramer and Shoup. We gain a number of benefits from this abstraction. First, we obtain a modular protocol that can be described using just three high-level cryptographic tools. This allows a simpl ...

Keywords: Passwords, authentication, dictionary attack, projective hash functions

4 Authentication and biometrics: Fortifying password authentication in integrated healthcare delivery systems

Yanjiang Yang, Robert H. Deng, Feng Bao

March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**

Publisher: ACM

Full text available: pdf(414.06 KB) Additional Information: full citation, abstract, references, index terms

Integrated Delivery Systems (IDSs) now become a primary means of care provision in healthcare domain. However, existing password systems (under either the single-server model or the multi-server model) do not provide adequate security when applied to IDSs. We are thus motivated to present a *practical* password authentication system built upon a novel two-server model. We generalize the two-server model to an architecture of a single *control server* supporting multiple *service serv ...*

Keywords: *dictionary attack, integrated delivery systems (IDSs), password system, user authentication and key exchange*

5 Federated databases and systems: part I --- a tutorial on their data sharing

David K. Hsiao

July 1992 **The VLDB Journal — The International Journal on Very Large Data Bases**, Volume 1 Issue 1

Publisher: Springer-Verlag New York, Inc.

Full text available: pdf(2.99 MB) Additional Information: full citation, abstract, references, citings

The issues and solutions for the interoperability of a class of heterogeneous databases and their database systems are expounded in two parts. Part I presents the data-sharing issues in federated databases and systems. Part II, which will appear in a future issue, explores resource-consolidation issues. *Interoperability* in this context refers to data sharing among heterogeneous databases, and to resource consolidation of computer hardware, system software, and support personnel. *Resour ...*

Keywords: *attribute-based, data-model-and-language-to-data-model-and-language mappings, database conversion, hierarchical, network, object-oriented, relational, schema transformation, transaction translation*

6 Separating key management from file system security

David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel

December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles SOSP '99**, Volume 33 Issue 5

Publisher: ACM Press

Full text available: pdf(1.77 MB) Additional Information: full citation, abstract, references, citings, index

terms

No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use.We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

7 Public-key cryptography and password protocols: the multi-user case

Maurizio Kliban Boyarsky
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**
Publisher: ACM Press

Full text available: pdf(1.00 MB) Additional Information: full citation, abstract, references, citings, index terms

The problem of password authentication over an insecure network when the user holds only a human-memorizable password has received much attention in the literature. The first rigorous treatment was provided by Halevi and Krawczyk, who studied off-line password guessing attacks in the scenario in which the authentication server possesses a pair of private and public keys. In this work we: Show the inadequacy of both the HK formalization and protocol in the ...

8 Authentication and passwords: Dynamic pharming attacks and locked same-origin policies for web browsers

Chris Karlof, Umesh Shankar, J. D. Tygar, David Wagner
October 2007 **Proceedings of the 14th ACM conference on Computer and communications security CCS '07**
Publisher: ACM

Full text available: pdf(504.43 KB) Additional Information: full citation, abstract, references, index terms

We describe a new attack against web authentication, which we call *dynamic pharming*. Dynamic pharming works by hijacking DNS and sending the victim's browser malicious Javascript, which then exploits DNS rebinding vulnerabilities and the name-based same-origin policy to hijack a legitimate session after authentication has taken place. As a result, the attack works regardless of the authentication scheme used. Dynamic pharming enables the adversary to eavesdrop on sensitive content, for ...

Keywords: pharming, same-origin policy, web authentication

9 Strong password-only authenticated key exchange

David P. Jablon
October 1996 **ACM SIGCOMM Computer Communication Review**, Volume 26 Issue 5
Publisher: ACM Press

Full text available: pdf(1.52 MB) Additional Information: full citation, abstract, citings, index terms

A new simple password exponential key exchange method (SPEKE) is described. It belongs to an exclusive class of methods which provide authentication and key establishment over an insecure channel using only a small password, without risk of offline dictionary attack. SPEKE and the closely-related Diffie-Hellman Encrypted Key Exchange (DH-EKE) are examined in light of both known and new attacks, along with sufficient preventive constraints. Although SPEKE and DH-EKE are similar, the constraints a ...

10 Operating system principles

Per Brinch Hansen
January 1973 Book
Publisher: Prentice-Hall, Inc.

Full text available: pdf(16.81 MB) Additional Information: full citation, abstract, references, cited by, index terms

From the Preface

MAIN GOAL

This book tries to give students of computer science and professional programmers a general understanding of *operating systems*--the programs that enable people to share computers efficiently.

To make the sharing of a computer tolerable, an operating system must enforce certain rules of behavior on all its users. One would therefore expect the designers of operating systems to do their utmost to make them as s ...

11 Final report of the ANSI/X3/SPARC DBS-SG relational database task group

July 1982 **ACM SIGMOD Record**, Volume 12 Issue 4
Publisher: ACM Press
Full text available: pdf(4.69 MB) Additional Information: full citation, citings

12 Interoperability of multiple autonomous databases

Witold Litwin, Leo Mark, Nick Roussopoulos
September 1990 **ACM Computing Surveys (CSUR)**, Volume 22 Issue 3
Publisher: ACM Press

Full text available: pdf(2.66 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Database systems were a solution to the problem of shared access to heterogeneous files created by multiple autonomous applications in a centralized environment. To make data usage easier, the files were replaced by a globally integrated database. To a large extent, the idea was successful, and many databases are now accessible through local and long-haul networks. Unavoidably, users now need shared access to multiple autonomous databases. The question is what the corresponding methodology ...

13 Attacking passwords and bringing down the network: Keyboard acoustic emanations revisited

Li Zhuang, Feng Zhou, J. D. Tygar
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press

Full text available: pdf(198.94 KB) Additional Information: full citation, abstract, references, citings, index terms

We examine the problem of keyboard acoustic emanations. We present a novel attack taking as input a 10-minute sound recording of a user typing English text using a keyboard, and then recovering up to 96% of typed characters. There is no need for a labeled training recording. Moreover the recognizer bootstrapped this way can even recognize random text such as passwords: In our experiments, 90% of 5-character random passwords using only letters can be generated in fewer than 20 attempts by an adve ...

Keywords: HMM, acoustic emanations, cepstrum, computer security, electronic

eavesdropping, hidden Markov models, human factors, keyboards, learning theory, privacy, signal analysis

14 On secure and pseudonymous client-relationships with multiple servers

Eran Gabber, Phillip B. Gibbons, David M. Kristol, Yossi Matias, Alain Mayer
November 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 4
Publisher: ACM Press

Full text available: pdf(161.56 KB) Additional Information: full citation, abstract, references, citings, index terms, review

This paper introduces a cryptographic engine, Janus, which assists clients in establishing and maintaining secure and pseudonymous relationships with multiple servers. The setting is such that clients reside on a particular subnet (e.g., corporate intranet, ISP) and the servers reside anywhere on the Internet. The Janus engine allows each client-server relationship to use either weak or strong authentication on each interaction. At the same time, each interaction preserves privacy by neithe ...

Keywords: Janus function, anonymity, mailbox, persistent relationship, privacy, pseudonym

15 GPGPU: general purpose computation on graphics hardware

David Luebke, Mark Harris, Jens Krüger, Tim Purcell, Naga Govindaraju, Ian Buck, Cliff Woolley, Aaron Lefohn
August 2004 **ACM SIGGRAPH 2004 Course Notes SIGGRAPH '04**
Publisher: ACM Press
Full text available: pdf(63.03 MB) Additional Information: full citation, abstract, citings

The graphics processor (GPU) on today's commodity video cards has evolved into an extremely powerful and flexible processor. The latest graphics architectures provide tremendous memory bandwidth and computational horsepower, with fully programmable vertex and pixel processing units that support vector operations up to full IEEE floating point precision. High level languages have emerged for graphics hardware, making this computational power accessible. Architecturally, GPUs are highly parallel s ...

16 Password management, mnemonics, and mother's maiden names: Passpet: convenient password management and phishing protection

Ka-Ping Yee, Kragen Sitaker
July 2006 **Proceedings of the second symposium on Usable privacy and security SOUPS '06**
Publisher: ACM Press
Full text available: pdf(479.35 KB) Additional Information: full citation, abstract, references, index terms

We describe Passpet, a tool that improves both the convenience and security of website logins through a combination of techniques. Password hashing helps users manage multiple accounts by turning a single memorized password into a different password for each account. User-assigned site labels (petnames) help users securely identify sites in the face of determined attempts at impersonation (phishing). Password-strengthening measures defend against dictionary attacks. Customizing the user interfac ...

17 Multilevel μTESLA: Broadcast authentication for distributed sensor networks

Donggang Liu, Peng Ning
November 2004 **ACM Transactions on Embedded Computing Systems (TECS)**, Volume 3 Issue 4
Publisher: ACM Press

Full text available: pdf(410.86 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Broadcast authentication is a fundamental security service in distributed sensor networks. This paper presents the development of a scalable broadcast authentication scheme named multilevel μTESLA based on μTESLA, a broadcast authentication protocol whose scalability is limited by its unicast-based initial parameter distribution. Multilevel μTESLA satisfies several nice properties, including low overhead, tolerance of message loss, scalability to large networks, and re ...

Keywords: Broadcast authentication, TESLA, sensor networks

18 Authentication in office system internetworks

Jay E. Israel, Theodore A. Linden
July 1983 **ACM Transactions on Information Systems (TOIS)**, Volume 1 Issue 3
Publisher: ACM Press
Full text available: pdf(1.28 MB) Additional Information: full citation, references, index terms

19 Distributed operating systems

Andrew S. Tanenbaum, Robbert Van Renesse
December 1985 **ACM Computing Surveys (CSUR)**, Volume 17 Issue 4
Publisher: ACM Press
Full text available: pdf(5.49 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Distributed operating systems have many aspects in common with centralized ones, but they also differ in certain ways. This paper is intended as an introduction to distributed operating systems, and especially to current university research about them. After a discussion of what constitutes a distributed operating system and how it is distinguished from a computer network, various key design issues are discussed. Then several examples of current research projects are examined in some detail ...

20 Secure sessions for Web services

Karthikeyan Bhargavan, Ricardo Corin, Cédric Fournet, Andrew D. Gordon
May 2007 **ACM Transactions on Information and System Security (TISSEC)**, Volume 10 Issue 2
Publisher: ACM Press
Full text available: pdf(579.98 KB) Additional Information: full citation, abstract, references, index terms

We address the problem of securing sequences of SOAP messages exchanged between web services and their clients. The WS-Security standard defines basic mechanisms to secure SOAP traffic, one message at a time. For typical web services, however, using WS-Security independently for each message is rather inefficient; moreover, it is often important to secure the integrity of a whole session, as well as each message. To these ends, recent specifications provide further SOAP-level mechanisms. WS-S ...

Keywords: Web services, XML security

Terms used: **key password biometric multiple several different** Found **214** of **216,412**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 Authentication and biometrics: Fortifying password authentication in integrated healthcare delivery systems
Yanjiang Yang, Robert H. Deng, Feng Bao
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**
Publisher: ACM
Full text available: pdf(414.06 KB) Additional Information: full citation, abstract, references, index terms

Integrated Delivery Systems (IDSs) now become a primary means of care provision in healthcare domain. However, existing password systems (under either the single-server model or the multi-server model) do not provide adequate security when applied to IDSs. We are thus motivated to present a *practical* password authentication system built upon a novel two-server model. We generalize the two-server model to an architecture of a single *control server* supporting multiple *service serv ...*

Keywords: *dictionary attack, integrated delivery systems (IDSs), password system, user authentication and key exchange*

2 Security, privacy and anonymity: Privacy preserving multi-factor authentication with biometrics
Abhilasha Bhargav-Spantzel, Anna Squicciarini, Elisa Bertino
November 2006 **Proceedings of the second ACM workshop on Digital identity management DIM '06**
Publisher: ACM Press
Full text available: pdf(228.45 KB) Additional Information: full citation, abstract, references, index terms

An emerging approach to the problem of reducing the identity theft is represented by the adoption of biometric authentication systems. Such systems however present however several challenges, related to privacy, reliability, security of the biometric data. Inter-operability is also required among the devices used for the authentication. Moreover, very often biometric authentication in itself is not sufficient as a conclusive proof of identity and has to be complemented with multiple other proofs ...

Keywords: authentication, biometrics, identity theft prevention, privacy

3 Attacking passwords and bringing down the network: Keyboard acoustic emanations

revisited
Li Zhuang, Feng Zhou, J. D. Tygar
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press

Full text available: pdf(198.94 KB) Additional Information: full citation, abstract, references, citings, index terms

We examine the problem of keyboard acoustic emanations. We present a novel attack taking as input a 10-minute sound recording of a user typing English text using a keyboard, and then recovering up to 96% of typed characters. There is no need for a labeled training recording. Moreover the recognizer bootstrapped this way can even recognize random text such as passwords: In our experiments, 90% of 5-character random passwords using only letters can be generated in fewer than 20 attempts by an adve ...

Keywords: HMM, acoustic emanations, cepstrum, computer security, electronic eavesdropping, hidden Markov models, human factors, keyboards, learning theory, privacy, signal analysis

4 National id card: the next generation: The US/Mexico border crossing card (BCC): a case study in biometric, machine-readable id
Andrew Schulman
April 2002 **Proceedings of the 12th annual conference on Computers, freedom and privacy CFP '02**
Publisher: ACM Press
Full text available: htm(187.31 KB) Additional Information: full citation, index terms

5 Face recognition: A literature survey
W. Zhao, R. Chellappa, P. J. Phillips, A. Rosenfeld
December 2003 **ACM Computing Surveys (CSUR)**, Volume 35 Issue 4
Publisher: ACM Press

Full text available: pdf(4.28 MB) Additional Information: full citation, abstract, references, citings, index terms

As one of the most successful applications of image analysis and understanding, face recognition has recently received significant attention, especially during the past several years. At least two reasons account for this trend: the first is the wide range of commercial and law enforcement applications, and the second is the availability of feasible technologies after 30 years of research. Even though current machine recognition systems have reached a certain level of maturity, their success is ...

Keywords: Face recognition, person identification

6 Authentication using graphical passwords: effects of tolerance and image choice
Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, Nasir Memon
July 2005 **Proceedings of the 2005 symposium on Usable privacy and security SOUPS '05**
Publisher: ACM Press

Full text available: pdf(555.83 KB) Additional Information: full citation, abstract, references, citings, index terms

Graphical passwords are an alternative to alphanumeric passwords in which users click on

images to authenticate themselves rather than type alphanumeric strings. We have developed one such system, called PassPoints, and evaluated it with human users. The results of the evaluation were promising with respect to rmemorability of the graphical password. In this study we expand our human factors testing by studying two issues: the effect of tolerance, or margin of error, in clicking on the password ...

Keywords: PassPoints, authentication, graphical passwords, human factors, password images, password security, tolerance, usable security

7 Smart Cards and Biometrics: The cool way to make secure transactions

David Corcoran, David Sims, Bob Hillhouse
March 1999 **Linux Journal**
Publisher: Specialized Systems Consultants, Inc.
Full text available: html(22.95 KB) Additional Information: full citation, index terms

8 A fuzzy commitment scheme

Ari Juels, Martin Wattenberg
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**
Publisher: ACM Press
Full text available: pdf(966.08 KB) Additional Information: full citation, abstract, references, citings, index terms

We combine well-known techniques from the areas of error-correcting codes and cryptography to achieve a new type of cryptographic primitive that we refer to as a fuzzy commitment scheme. Like a conventional cryptographic commitment scheme, our fuzzy commitment scheme is both concealing and binding: it is infeasible for an attacker to learn the committed value, and also for the committer to decommit a value in more than one way. In a convent ...

9 Research contibutions: A review of information security issues and respective research contributions

Mikko T. Siponen, Harri Oinas-Kukkonen
February 2007 **ACM SIGMIS Database**, Volume 38 Issue 1
Publisher: ACM Press
Full text available: pdf(353.82 KB) Additional Information: full citation, abstract, references, index terms

This paper identifies four security issues (access to Information Systems, secure communication, security management, development of secure Information Systems), and examines the extent to which these security issues have been addressed by existing research efforts. Research contributions in relation to these four security issues are analyzed from three viewpoints: a meta-model for information systems, the research approaches used, and the reference disciplines used. Our survey reveals that most ...

Keywords: computer science

10 Network-based approach: Modeling cryptographic properties of voice and voice-based entity authentication

Giovanni Di Crescenzo, Munir Cochinwala, Hyong S. Shim
November 2007 **Proceedings of the 2007 ACM workshop on Digital identity management DIM '07**
Publisher: ACM

Full text available: pdf(230.76 KB) Additional Information: full citation, abstract, references, index terms

Strong and/or multi-factor entity authentication protocols are of crucial importancein building successful identity management architectures. Popular mechanisms to achieve these types of entity authentication are biometrics, and, in particular, voice, for which there are especially interesting business cases in the telecommunication and financial industries, among others. Despite several studies on the suitability of voice within entity authentication protocols, there has been little or no fo ...

Keywords: biometrics, entity authentication, modeling human factors, voice

11 Identification and authentication when users have multiple accounts

W. R. Shockley

August 1993 **Proceedings on the 1992-1993 workshop on New security paradigms NSPW '92-93**

Publisher: ACM Press

Full text available: pdf(788.71 KB) Additional Information: full citation, references

12 Poster session 2: Password management using doodles

Naveen Sundar Govindarajulu, Sriganesh Madhvanath

November 2007 **Proceedings of the 9th international conference on Multimodal interfaces ICMI '07**

Publisher: ACM

Full text available: pdf(239.75 KB) Additional Information: full citation, abstract, references, index terms

The average computer user needs to remember a large number of text username and password combinations for different applications, which places a large cognitive load on the user. Consequently users tend to write down passwords, use easy to remember (and guess) passwords, or use the same password for multiple applications, leading to security risks. This paper describes the use of personalized hand-drawn "doodles" for recall and management of password information. Since doodles can be easier t ...

Keywords: doodles, password management

13 Applications I: Secure fingerprint-based authentication for Lotus Notes®

Nalini K. Ratha, Jonathan H. Connell, Ruud M. Bolle

October 2001 **Proceedings of the 2001 workshop on Multimedia and security: new challenges MM&Sec '01**

Publisher: ACM Press

Full text available: pdf(731.41 KB) Additional Information: full citation, abstract, references

Fingerprints have been used to recognize people for several decades. The advent of low cost inkless fingerprint scanners coupled with extra compute power available in client workstations, biometrics in general and fingerprints in particular are being considered for many secure authentication applications. Lotus Notes is a groupware supporting email access and other activities such as calendar management included in it. In this paper, we describe the architecture of a system that integrates bo ...

14 Audio-visual multimodal fusion for biometric person authentication and liveness verification

Girija Chetty, Michael Wagner

April 2006 **Proceedings of the 2005 NICTA-HCSNet Multimodal User Interaction Workshop - Volume 57 MMUI '05**

Publisher: Australian Computer Society, Inc.
Full text available: pdf(719.65 KB) Additional Information: full citation, abstract, references, index terms

In this paper we propose a multimodal fusion framework based on novel face-voice fusion techniques for biometric person authentication and liveness verification. Checking liveness guards the system against spoof/replay attacks by ensuring that the biometric data is captured from an authorised live person. The proposed framework based on bi-modal feature fusion, cross-modal fusion as well as 3D shape and texture fusion techniques, allow a significant improvement in system performance against impo ...

Keywords: biometric authentication, liveness verification, multimodal fusion

15 Authentication: Pass-thoughts: authenticating with our minds

Julie Thorpe, P. C. van Oorschot, Anil Somayaji
September 2005 **Proceedings of the 2005 workshop on New security paradigms NSPW '05**
Publisher: ACM Press
Full text available: pdf(3.94 MB) Additional Information: full citation, abstract, references

We present a novel idea for user authentication that we call *pass-thoughts*. Recent advances in Brain-Computer Interface (BCI) technology indicate that there is potential for a new type of human-computer interaction: a user transmitting thoughts directly to a computer. The goal of a pass-thought system would be to extract as much entropy as possible from a user's brain signals upon "transmitting" a thought. Provided that these brain signals can be recorded and processed in an accurate and ...

Keywords: authentication, passwords

16 The domino effect of password reuse

Blake Ives, Kenneth R. Walsh, Helmut Schneider
April 2004 **Communications of the ACM**, Volume 47 Issue 4
Publisher: ACM Press
Full text available: pdf(100.88 KB) html(23.20 KB) Additional Information: full citation, abstract, references, citings, index terms

One weak spot is all it takes to open secured digital doors and online accounts causing untold damage and consequences.

17 Password hardening based on keystroke dynamics

Fabian Monrose, Michael K. Reiter, Susanne Wetzel
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**
Publisher: ACM Press
Full text available: pdf(1.01 MB) Additional Information: full citation, abstract, references, citings, index terms

We present a novel approach to improving the security of passwords. In our approach, the legitimate user's typing patterns (e.g., durations of keystrokes, and latencies between keystrokes) are combined with the user's password to generate a hardened password that is convincingly more secure than conventional passwords against both online and offline attackers. In addition, our scheme automatically adapts to gradual changes in a user's typing patterns while maintaining the s ...

18 Invited Talks: Secure information sharing enabled by Trusted Computing and PEI models

Ravi Sandhu, Kumar Ranganathan, Xinwen Zhang
March 2006 **Proceedings of the 2006 ACM Symposium on Information, computer and communications security ASIACCS '06**
Publisher: ACM Press
Full text available: pdf(210.37 KB) Additional Information: full citation, abstract, references, index terms

The central goal of secure information sharing is to "share but protect" where the motivation to "protect" is to safeguard the sensitive content from unauthorized disclosure (in contrast to protecting the content to avoid loss of revenue as in retail Digital Rights Management). This elusive goal has been a major driver for information security for over three decades. Recently, the need for secure information sharing has dramatically increased with the explosion of the Internet and the convergenc ...

Keywords: PEI models, access control, authorization, secure information sharing, security framework, trusted computing

19 Voice biometrics
Judith A. Markowitz
September 2000 **Communications of the ACM**, Volume 43 Issue 9
Publisher: ACM Press
Full text available: pdf(240.49 KB) html(36.88 KB) Additional Information: full citation, references, citings, index terms

20 Protecting applications with transient authentication
Mark D. Corner, Brian D. Noble
May 2003 **Proceedings of the 1st international conference on Mobile systems, applications and services MobiSys '03**
Publisher: ACM Press
Full text available: pdf(294.40 KB) Additional Information: full citation, abstract, references, cited by

How does a machine know who is using it? Current systems authenticate their users infrequently, and assume the user's identity does not change. Such *persistent authentication* is inappropriate for mobile and ubiquitous systems, where associations between people and devices are fluid and unpredictable. We solve this problem with *Transient Authentication*, in which a small hardware token continuously authenticates the user's presence over a short-range, wireless link. We present the fo ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	6	"6230272".pn. "6035398".pn. "6311272".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 13:49
S2	1	"6035398".pn.	USPAT	OR	OFF	2006/08/30 21:44
S3	1	"6311272".pn.	USPAT	OR	OFF	2006/09/01 18:36
S4	260	digital adj rights adj management	USPAT	OR	OFF	2006/09/01 18:36
S5	50	digital adj rights adj management and (content adj key)	USPAT	OR	OFF	2006/09/01 18:36
S6	0	digital adj rights adj management and (content adj key) and hurtado. in.	USPAT	OR	OFF	2006/09/01 18:37
S7	63	hurtado.in.	USPAT	OR	OFF	2006/09/01 18:37
S8	0	digital adj rights adj management and (content adj key) and hurtado. in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/01 18:37
S9	204	hurtado.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/01 18:37
S10	0	hurtado.in. and (digital adj right) and (secure adj container)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/09/01 18:37
S11	4	hurtado.in. and (digital adj right) and (secure adj container)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/09/01 18:37
S12	6	"5805801".pn. "5489896".pn. "5935245".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/05/09 13:52

EAST Search History

S13	97	(password$2 biometric$2) with (multiple$2) with (key$2) with (encrypt$4 encod$3 encipher$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:00
S14	67	HAMID near2 LAURENCE.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:00
S15	5	HAMID near2 LAURENCE.in. and (password).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:09
S16	196	activcard.as.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:09
S17	39	activcard.as. and (password$2 biometric$2).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:10
S18	8	activcard.as. and (password$2 biometric$2).clm. and (key).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:14
S19	2088	713/193.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:17
S20	505	713/166.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:17

EAST Search History

S21	948	713/186.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:23
S22	904	726/27.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:23
S23	4226	S19 S20 S21 S22	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:24
S24	5	S23 and (password$2 biometric$2) with (multiple$2) with (key$2) with (encrypt$4 encod$3 encipher$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:24
S25	2087	S23 and (password$2 biometric$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:24
S26	1202	S23 and (password$2 biometric$2) and (key$2) with (encrypt$4 encod$3 encipher$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:25
S27	257	S23 and (password$2 biometric$2) and (key$2) with (encrypt$4 encod$3 encipher$2) and (different$2 multipl$3 several$2) near3 (password$2 biometric$2 (authorization$2 near2 process$2))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:50
S28	3010	S23 and (authoriz$5 authenticat$5) and (key$2 password$2 biometric$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 14:54

EAST Search History

S29	530	S23 and (authoriz$5 authenticat$5) and (key$2 password$2 biometric$3) and (different$4 multiple$2) with (biometric$2 password$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 15:07
S30	186	S23 and (authoriz$5 authenticat$5) and (key$2 password$2 biometric$3) and (different$4 multiple$2) with (biometric$2 password$2) and ((smart adj card) (IC adj card))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 15:08
S31	400	726/9.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 15:08
S32	212	726/20.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 15:08
S33	4714	S31 S32 S23	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 15:08
S34	5	S33 and (password$2 biometric$2) with (multiple$2) with (key$2) with (encrypt$4 encod$3 encipher$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 15:10
S35	10	S33 and (multiple$2 different) with (authorization$2 near2 process$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/05 15:10
S36	2088	713/193.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/06 15:15

EAST Search History

S37	505	713/166.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/06 15:15
S38	948	713/186.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/06 15:15
S39	904	726/27.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/06 15:15
S40	4226	S36 S37 S38 S39	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/06 15:15
S41	400	726/9.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/06 15:15
S42	212	726/20.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/06 15:15
S43	4714	S41 S42 S40	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/06 15:15
S44	282	S43 and (password$2 biometric$2) and (key$2) with (encrypt$4 encod$3 encipher$2) and (different$2 multipl$3 several$2) near3 (password$2 biometric$2 (authorization$2 near2 process$2))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/06 15:16

EAST Search History

S45	5	S43 and (password$2 biometric$2) with (multiple$2) with (key$2) with (encrypt$4 encod$3 encipher$2)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/06 15:17
S46	15	S43 and (multiple$2 with authorization).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/06 15:17
S47	99	S43 and ((different multiple) with (password$2 biometric)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/06 15:19